Business Continuity Management

Exploiting agility in an uncertain world

Overview


This White Paper outlines all you need to know about Business Continuity Management; about the importance of having a resilient and agile organisation in an uncertain business world.

It explains the business benefits of Business Continuity Management along with the technical and organisational considerations that are needed to deploy it. And how BT can help you protect your business operations with seamless continuity and systems agility through world-class IP infrastructure solutions and consultancy.
Contents

Overview ......................................................................................................................... 1

Introduction .................................................................................................................... 3

Understanding Business Continuity Management ............................................................ 4
  You cannot predict the environment .............................................................................. 4
  Conditions Favour Agility ............................................................................................... 5

People and Processes .................................................................................................... 6
  Deploying Business Continuity Management .................................................................. 6
  BT’s Capability .............................................................................................................. 7

Infrastructure ................................................................................................................ 8
  Optical Connectivity ..................................................................................................... 9
    BT’s Capability ........................................................................................................... 9
  Storage .......................................................................................................................... 10
    BT’s Capability .......................................................................................................... 11
  Security ......................................................................................................................... 11
    BT’s Capability ........................................................................................................... 12-13
  Desktop and Office ...................................................................................................... 14
  Summary ....................................................................................................................... 14
**Introduction**

“…(Board) policies should take account of the risks faced by the company, its risk appetite, the controllability of the risks and the cost/benefit of the controls identified. The control system should be embedded and responsive, it should include procedures for reporting failures and weaknesses, together with the corrective action taken.”

- From The Turnbull Report, Guidance on Internal Control. Produced by the Institute of Chartered Accountants in England & Wales (ICAEW), September 1999.

The requirements laid down by The Turnbull Report to identify business risks and impacts puts increased pressure on all organisations. And all at a time when complex IT systems have never been more critical to maintaining business operations: the days of the simple Disaster Recovery plan are gone.

Business Continuity is a discipline that takes up significant resources and is one that organisations often find difficult to develop and support on a continuing basis. Changing business drivers and new technologies require current and tested solutions to be maintained to ensure business continuity in critical operational areas.

This White Paper shows it is not possible to predict the impact of environmental change and demonstrates that it is only the technologically agile businesses which will best respond to it. Our solution to building you an agile and resilient business is BT Business Continuity Management and here we demonstrate how BT can help you become – and stay – responsive to change.

There is one key and fundamental element that underpins business resilience and that is the IT infrastructure. More importantly, there is only one element that can tie that network infrastructure together – and that is IP Infrastructure. IP Infrastructure supports the office and IP Infrastructure supports the data centre: IP Infrastructure *is* the network and the network *is* the computer.

Increasingly the network itself is also absorbing important elements that were previously located in the office or data centre – for instance, storage area networking (SAN), hosted applications and server farms.

So the starting point for Business Continuity has to be the business of management: management responsibility as defined by Turnbull, management execution to ensure risk assessment is carried out, that appropriate plans are made and that these are tested in a robust manner and on a regular basis. To help management address these responsibilities, BT has defined three stages that this paper investigates in further detail:

- Understanding Business Continuity Management
- People & Processes
- Infrastructure
Understanding Business Continuity Management

You cannot predict the environment

The environment is unpredictable. Organisations, regardless of their size, can suffer crisis and disaster at any time and from any number of sources. These sources of disruption can vary from a natural fire or flood, to a technical system failure, deliberate hacking or even a politically motivated attack.

Such incidents can cause interruption to mission critical functions and processes as well as damaging reputation and brand name.

To indicate the sources of disruption organisations can suffer the Chartered Institute of Management conducted a survey of over 150 managers in February 1999 and again in February 2002. This is what they found:

As you can see from the graph above, the results of the survey indicated that organisations suffered a number of different disruptions.

The largest disruption was caused due to a loss of skills: this affected almost 35 per cent of organisations, rising from only one per cent in 1999. Interestingly the survey also showed that 18 per cent of organisations had incurred disruption due to flooding and that 2 per cent had suffered some sort of terrorist attack.

This is important to bear in mind in terms of developing a business continuity strategy. Organisations may well be making a mistake by focusing on terrorism and the events of September 11th, as they usually constitute a wholly unpredictable event. In terms of business continuity management (BCM), there are more immediate and less dramatic issues.

In many cases it is often the mundane things like poor cabling or power supply that cause the biggest problems. But they can have just as much of an impact on a company’s ability to deliver uninterrupted services as those of our worst nightmares.

For example a survey carried by Guardian IT suggested that companies in the City of London were 40 times more likely to suffer disasters and interruptions to their business as a result of the efforts of their plumbers than from terrorists.

The implications of business disruption to the organisation can be huge. For example in March 2002, Barclays Bank suffered an IT system fault on the eve of a bank holiday weekend that caused widespread disruption to the overnight processing of payments. This caused a huge loss of integrity to the company as well as damage to customer service and the company brand. In June 2001, the New York Stock Exchange had to stop trading for over one hour because of a failed software upgrade problem, causing stock listings and trading to be suspended.

Further back in August 1999, The Development Bank of Singapore experienced a system overload that caused processing errors, incorrect debiting at retail POS. The result? Acute embarrassment, loss of integrity and additional interest charges.

Of course, it’s never a problem, until it happens. But you can be ready.
Conditions Favour Agility

These uncertain environmental conditions favour organisations that have the necessary agility to meet the changing needs of customers and the marketplace regardless of any operational issues it may face.

The Business Continuity Institute defines business Continuity Management as:

“…the act of anticipating incidents which will affect mission critical functions and processes for the organisation and ensuring that it responds to any incident in a planned and rehearsed manner…”

The adoption of robust BCM can allow organisations to identify, manage and respond to disruption in a way that ultimately ensures the success and survival of the organisation.

But successful BCM must include not only the right technology infrastructure but also the right processes and people. At a fundamental level, it must be embedded into an organisation’s culture and strategic objectives.

Clearly, it is vital for an organisation to have a workable BCM strategy. If disaster strikes and an organisation can’t recover in a timely fashion, the consequences can include loss of revenue, defection of customers, deterioration of brand equity and permanent loss of shareholder value.

Organisations also have a legal requirement to put in place BCM. Recent government regulation on corporate governance now brings risk management and BCM into the scope of directors’ legal duties. The Turnbull report, commissioned by the Government as part of their review of company law states that:

“…an organisation must have a sound system of internal control dependant on a thorough and regular evaluation of the nature and extent of the risks to which it is exposed…”

Despite this, many companies are not doing enough to ensure their own continuity. A recent report produced by the Chartered Management Institute indicates that less than half of all organisations have a business continuity plan. Of that, only 57 per cent test it at least annually to make sure it works.

Further evidence shows that every five years, 20 per cent of companies suffer a major disruption through fire, flood, storm, power failure, hardware/software failures or deliberate attack. Of those companies which do not have business continuity plans, more than 40 per cent cease operations within two years.

In today’s competitive market, can you really afford to take that risk?

At BT, we manage some of the largest multimedia corporate networks in Europe – including our own. We have the experience, the expertise and the R&D to help you design, deploy and manage successful business continuity through the effective combination of People, Process and Infrastructure.
People and Processes

Deploying Business Continuity Management

Thorough business continuity management involves more than just Infrastructure. It must:
• be linked to management and strategic objectives
• be embedded into the existing processes and culture of the organisation

Critical steps to ensure this can be summarised as follows:

1. Assessment of ‘where your business is now’. This includes initial Risk Assessment and Impact Analysis, taking the business impact as the first priority.

2. Development of a Business Continuity Strategy, based on your legal and regulatory requirements and in the context of the technical Risk Assessment and Impact Analysis.

3. Implementation of all the steps towards building, maintaining and testing appropriate solutions to take them forward safely into the future.

4. Validation through effective project management of change processes and, most importantly, design and implementation of test schedules.

Like your company, BT has had to face these issues and implement appropriate safeguards across a scale of operation matched by very few other organisations. At the centre of this experience is the recognition that Organisational Strategy needs both to be accommodated – and accommodate – the rigors and discipline of Business Continuity Management.

Key learning from our own implementation is the recognition that three considerations need to be assessed in order to optimise the risk profile:

• Prevention: through the definition and deployment of robust security measures against cyber attack and unauthorised physical access.
• Mitigation: by limiting the potential impact resulting from a single incident – from the design stage onwards.
• Recovery: by ensuring appropriate facilities are available both technically and in terms of accommodation.
**BT's Capability**

Our capabilities stem from our unrivalled networking experience: BT carries 80 per cent of all credit card transactions in the UK as part of an estimated £70bn of funds transferred each day. We also provide the networks that transport other high value financial transactions, such as settleNET in the City.

Our high standards of expertise in network and security operations are further enhanced by the fact that 18 of the top 20 largest financial institutions have either outsourced their communications to BT – or we manage substantial, key elements of their infrastructure. These institutions' networks are part of over 40,000 that BT manages on behalf of customers in all sectors of business and government.

Increasingly, these payment environments are being extended to take full advantage of open networks – including the Internet – and BT works with its customers and strategic partners to reach high security standards. As part of a security structure, BT can provide expertise in the areas of: PKI (Digital Certificates) and encryption techniques between networks and desktop-to-desktop.

BT is heavily engaged in shaping the future of security.

We are a member of FIRST (Forum of Incident Response and Security Teams) and CERT (Computer Emergency Response Team), a security forum funded primarily by the US Department of Defense.

This experience places BT in a position to offer consultancy services (either on our own or with business partners) that will deliver the BCM components outlined above. We can also design and deliver the infrastructure required to meet the exacting standards of a global, 24-7 digital economy and give you service level guarantees through our outsourcing and managed services divisions.

BT also has the capability of a 24 x 7 Command Centre:

- monitoring, support and problem management for systems, storage and disaster recovery
- a Major Incident Team that manages the whole control and communication process from major failure alert, communication with senior managers/customers/affected site/recovery site/suppliers through to restoration of service and Business As Usual from the recovery site.

The services include the whole process of risk/impact assessment, development of solutions, implementation, production of recovery plans, testing, issue management, maintenance and actual recovery following an invocation.

BT can offer all of the advisory and consultancy services above, enabling businesses to build business continuity management and solutions based on their legal and regulatory requirements – according to properly assessed risks and impacts of failure. BT can help manage all the steps towards building, maintaining and testing appropriate solutions to take organisations forward into the future: safely.
**Infrastructure**

In order to deliver business continuity management and business agility you first need the right infrastructure in place. In short, I before E (I before Everything).

BCM is created by having a secure and dependable infrastructure: this includes both your voice and IP networks as well as your physical office facilities.

And to get there, you need the following:

- Ultra fast and scalable bandwidth to transport data
- Ability to mirror, store and retrieve your data
- A resilient network and operational office space
- All protected by specialist security tools
- Optical Connectivity
- Data Storage Portfolio
- Desktop and Office
- Security

Let’s look at how BT can deliver each of these requirements.
Connectivity

A vital prerequisite in delivering successful BCM is ensuring that organisations have the right network connectivity in place. The connectivity needs to be reliable and resilient.

BT can deliver connectivity into our customer’s premises by a number of ways, including private circuits and ISDN.

Optical connectivity is the next stage in network technology that will provide more bandwidth at a reduced cost to customers. It is a movement away from very complex, old networking technologies to much simpler and much cheaper networking technologies.

Optical is about providing ultra broadband speeds across the enterprise network with high volume and low cost. The benefits to customers will include more bandwidth at reduced cost, faster response times, services flexibility and a fundamental change in computing services models.

It is a key enabler for business continuity management as it allows the real time transport, storage and recovery of data, applications and mission critical systems. It can enable customers to transport large amounts of data off their site very quickly and provide the vital connectivity to BT’s unique data storage portfolio. In light of any disruption to the organisation, the deployment of optical connectivity can reduce downtime and minimise risk to the organisation.

BT now provides optical connectivity within its Wavestream Portfolio which provides our customers with yet another evolutionary step along the solutions roadmap, with full interoperability between existing WAN and LAN solutions.

Our optical reach is extensive and fully national: BT has the largest installed fibre infrastructure of any UK carrier – the map above shows just a top level view of one of our major network layers. It would be impossible to show all it all one map but we offer essentially complete coverage of mainland UK.

BT’s Capability

We have a comprehensive solution in place today:
- Extensive fibre availability nationwide.
- Wavestream Portfolio: gigabit connectivity (up to 40 gig per second)
- SHDS Solutions: slower speeds (up to one gig per second)
Storage

The digital economy is generating unprecedented amounts of data. Every click, every call and every enquiry generates data – and the explosion of rich media within the working environment has an exponential effect on storage requirements. This data needs to be stored: but to realise this information as a positive business asset, it must be fully protected, easily managed, easily accessible and be easily shared across the entire enterprise.

Recovering business, not applications.

Continuity has traditionally revolved around restoring a small number of key applications, but that model no longer does justice to the complexity and importance of today’s IT-driven business operations. Applications no longer exist in isolation, but are instead interconnected and interdependent. In addition, applications such as e-mail that were previously not considered to be mission critical, now most definitely are.

The only way to ensure resilience and continuity today to consolidate at the information layer and then use the technologies available to mirror that data to a second site. This is the difference between achieving true business continuity as opposed to just ad hoc recovery.

Eliminating Risk

The primary reason for deploying a business continuance strategy is to eliminate risk — and the threat of it – from the organisation. With the cost of downtime estimated at anywhere up to $400,000 per hour (AMR Research), business continuance is essential. When selecting resilience suppliers, customers must look for experience and expertise. Activated in a live crisis environment on over 11,000 occasions since its introduction, EMC’s SRDF remote mirroring software took eight years to develop: a proven recovery solution, it was vindicated most recently by the tragic events of September 11th:

“…Stock market trading resumed last Monday, in good part thanks to the duplicate data storage allowed by the products of EMC…”

– Barron’s Weekly, September 24, 2001

Business Continuity, not Disaster Recovery

Within most businesses, blame for the majority of downtime can still be laid at the door of ‘planned-for’ outages such as backup and reporting. With EMC’s software tools, enterprises can now create Business Continuance Volumes – extra copies of data created in real time – that allow these processes to be carried out in parallel, thus creating true business continuance in real-time. The added advantage of this type of approach is that BCVs also provide the instant restoration of data in the case of a disaster.
BT has entered the storage service provider (SSP) market with a comprehensive range of storage services that address a wide range of customer needs. Today, we offer a range of dedicated storage network solutions, drawn from our own solutions portfolio:

- Short Haul Data Servers for Fibre Channel.
- Metrowave DWDM services for Fibre Channel, ESCON etc.
- Business Quality MPLS QoS enabled IP services for storage solutions.

... as well as from those of our ‘best-of-breed’ partners:

- BT is a platinum EMC partner for the delivery of storage solutions.
- Additional partnerships with world class suppliers such as DELL, StorageTek and Veritas.

**BT’s Capability**

The figures below demonstrate the extensive scope of our resilience operations:

**Scale**
- Each week, 52 weeks a year, we back up over 200 terabytes of data for internal and external customers.
- And we manage over 200 terabytes (400 terabytes raw) of disk storage and over one and a half petabytes of data stored on tape.

**Experience**
- In 2001, we created 145 new disaster fallback solutions and performed over 50 system fallback rehearsals.
- Over 600 servers were configured for backup in one year.
- We implemented over 40 Storage Attached Network (SAN) configurations.

**Security**

Security is another key component for business resilience that, applied correctly, can provide the safe and profitable conduct of an organisation in a potentially hostile and uncertain environment. Organisations today have to defend themselves against a multiplicity of security issues, ranging from viruses, worms, fraud and other forms of attack. These security issues cost organisations billions of dollars every year through lost revenue and damage to business credibility and reputation; and the frequency and impact of these attacks continues to rise.

Because of the impact of security issues on organisations, it has now become a board level responsibility and a major investment decision.

It couldn’t be clearer: the Turnbull Report, quoted earlier, explicitly outlines the legal responsibilities of directors with regard to security. Furthermore, the government also expects organisations to follow the BS7799 standard for Information Security Management Systems.
Security practices should be contained within a group Security Policy that also feeds into Disaster Recovery and Business Continuity Management planning. The Security Policy needs to be a “living” document that is initially benchmarked against industry and International Standards (BS7799 or similar). Once the standards have been achieved it is important to maintain ongoing vigilance and ensure that your employees are aware of the policy, are aware of their own responsibilities and how the strategy affects them in the work.

BT has extensive experience in security: we help many organisations to create strong business practices for controlling security risks. This involves guiding organisations through a process that will help them reach the highest industry standards – and then maintain them.

**BT's Capability**

The BT approach to achieving an effective and appropriate risk management capability is based upon three key stages:

- **Benchmarking:** assessment of the existing level of risk exposure, and the ability of existing security processes and controls to appropriately manage risk.

- **Certification:** development and implementation of an appropriate and cost-effective risk reduction strategy, in accordance with best practice industry standards. For example, the BS7799 Specification for Information Security Management Systems, backed by additional requirements relating to Corporate Governance and various regulatory and legal issues.

- **Vigilance:** maintenance of an ongoing effective risk management posture and capability that reflects changing business activities, market developments, technological advances and legal and regulatory changes.

Our approach addresses security management through a combination of understanding the business risks attached to the use of new technology, coupled with a solid grasp of the risks associated with specific technological solutions.

A typical approach by BT would be through BT's IT-Security consultancy service and this is how we typically consult with our customers:

- Formal discussions with senior management to explore areas of risk and exposure.
- Assess and review processes and benchmarking.
- Consult, agree and create a core security strategy to meet agreed standards.
- Agree and create a methodology and implementation practice for continuous vigilance, testing and development.
This approach is based on creating long-term resilience to threats and creating internal best practices that customers can easily manage.

As the widely-respected R&D division of BT Group, BTexact Security Technologies has many years experience in the analysis of security risks, the design of solutions to minimise those security risks and in the audit of compliance against best-practice security standards. This experience has included the networks and services of BT’s customers and of BT: this includes major financial institutions and networks that are designated as part of the UK's Critical National Infrastructure.

BTexact is a developer of leading security standards, including IETF Internet security standards and 3G mobile security standards. It also plays a full role in the development of the BSI’s UK information security management standard BS7799 and its international counterpart ISO 17799. BTexact’s security practices are certified as meeting the standards of BS7799 and our penetration testing team has been approved by the UK Government IT Health CHECK scheme.

Our security practice offers a range of services that help you manage risks actively, together with a range of packaged solutions that use technology to improve your resilience to attack or breakdown.

The consultancy services include:
• Policy, including Risk Assessment, Audit and Due Diligence.
• Design and integration of secure solutions, including networks, systems and applications.
• Evaluation to quality and reduce exposure to attack, including network audits and penetration testing.
• Assurance to ensure that your business can operate effectively and profitably, while appropriately addressing security risks.

In addition to BTexact's consultancy, we offer solutions that span the following areas:
• PKI and cryptographic solutions, ranging from integration and implementation of simple applications to a complete managed service.
• Wireless LAN, IPsec and VPN solutions that help to expand your network capabilities easily without compromising security.
• Secure web solutions, enabling you to trade online with confidence and inspire confidence within your customers.
• Firewall solutions, including product selection, testing and integration.
**Desktop and Office**

If fire or flood destroys your telecommunications system, it’s probable that your office or whole building could be damaged beyond immediate use. As a provider of a wide range of business continuity services, BT CommSure offers the use of both fixed and re-locatable recovery centres where business operations can be resumed ASAP.

Fixed Centres offer your company fully furnished and equipped premises in which to carry on business. Re-locatable centres allow your company to resume working as quickly as possible. Fully furnished, these centres meet permanent building design regulations.

**Summary**

In summary BT can deliver the IP Infrastructure and consultancy that enable organisations to build continuity plans and solutions based on their legal and regulatory requirements. This is according to properly assessed risks and impacts of failure and all the steps towards building, maintaining and testing appropriate solutions to take them forward safely into the future.

This can also extend to integration with non-IT plans for critical people, skills, and buildings to protect against single points of failure, making business continuity a Business As Usual activity throughout the enterprise.

There is no way to predict what will happen and when – but we have the technology, the resources, the experience and the expertise to help you proactively protect your business just when you need it most.

BT: in an uncertain world, we're all you need to know.